Economic Location-Based Services, Privacy and the Relationship to Identity

Lothar Fritsch, Johann Wolfgang Goethe – University Frankfurt am Main

***Abstract*—Mobile telephony and mobile internet are driving a new application paradigm: location-based services (LBS). Based on a person's location and context, personalized applications can be deployed. Thus, internet-based systems will continuously collect and process the location in relationship to a personal context of an identified customer. One of the challenges in designing LBS infrastructures is the concurrent design for economic infrastructures and the preservation of privacy of the subjects whose location is tracked. This presentation will explain typical LBS scenarios, the resulting new privacy challenges and user requirements and raises economic questions about privacy-design. The topics will be connected to "mobile identity" to derive what particular identity management issues can be found in LBS.**

***Index Terms*—communication systems privacy, location, privacy, security, infrastructures, wireless, economy, mobility**

I. Introduction

LOCATION awareness of networked application system started as a side-effect of mobile telephony. Today most LBS scenarios base on some form of navigation to a destination, or some form of fleet management or workforce scheduling. But mobile operators as Vodafone or T-Mobile prepare to position access to a mobile users' location data as a large-scale sales product. Thus, highly economic, scaling infrastructures are needed to deal with all questions of access, control, privacy protection and other aspects of mobile business. This article presents large-scale business models for LBS and discusses privacy questions that arise. Finally, the connection to identity management will be made by discussion mobility aspects of identity.

A. LBS – A growing Technology

Mobile Commerce applications differ from generic e-commerce applications in four properties [=133 - Turowski 2004 Mobile Commerce: Gru...=]:

Ubiquity / Reach ability enable applications to be used from anywhere, any time. *Context Sensitivity* supports applications provided for a particular context. *Identification / Personalization* takes advantage of mobile networks providing identity management technologies that enable personalized, authenticated, and paid-for personal applications. Finally, *Telemetry / 'Remote Control'* functions enable users to remotely control applications or processes.

Location based service applications are different from general Internet applications in two properties. First, mobility of the user and device lets a user or device accesses services from a variety of networks with changing network parameters and possible periods of no connectivity. Second, location sensitivity enables applications to process location information to add value to an application. We define business model as a high-level description of parties, their interactions and business processes with the purpose of value generation. But how do m-commerce business models look like? Giovanni Camponovo [1] describes a generic m-commerce model as a mesh of parties from infrastructure, service, technology, user, communication and regulation domains. As location based services are a special form of m-commerce, Camponovo's model also applies to them.

Location data for LBS is either provided by the communication network (e.g. a mobile phone network) or by specialized hardware at the user device (e.g. a beacon or a GPS receiver). Thus communication and technology players have the biggest influence on the communication and localization technology used. The location of a person is highly sensitive data. Thus regulation authorities have an interest in controlling its usage.

The actual location based services are offered by application providers. Due to their powerful position, mobile operators may act as localization and/or payment service providers, as portal operators or even as application providers themselves, thus impersonating different actors of the service domain.

B. Basic LBS Business Scenarios

Depending on what party does the localization and the service provisioning, LBS business models can be distinguished in to the scenarios in Fig.1:

- Mobile devices and application providers take care of localization and application processing. The mobile network is used as a data channel. This is the *direct localization scenario*.
- Mobile operator offers the localization and application. Here, we do not find any external application provider, because this is part of the operator's portal. This is the *operator-portal scenario*.

Manuscript received January 15, 2005. This work was supported by the EU IST PRIME and FIDIS projects; however, it represents the view of the author only.

Lothar Fritsch is a researcher in privacy-friendly location-based services at the Chair for M-Commerce & Multilateral Security at Johann Wolfgang Goethe-University, Gräfstraße 78, 60054 Frankfurt (tel. +49 69 79825301; fax: +49 69 79825306; e-mail: Lothar.Fritsch@M-Lehrstuhl.de).

- Mobile operators deliver communication and localization, but the LBS are provided by independent application providers. This is the *application provider scenario*.
- Intermediaries collect localization information from various sources (operators, GPS, WLAN), aggregate it and serve as a location broker for application providers. This is the *intermediary scenario.*

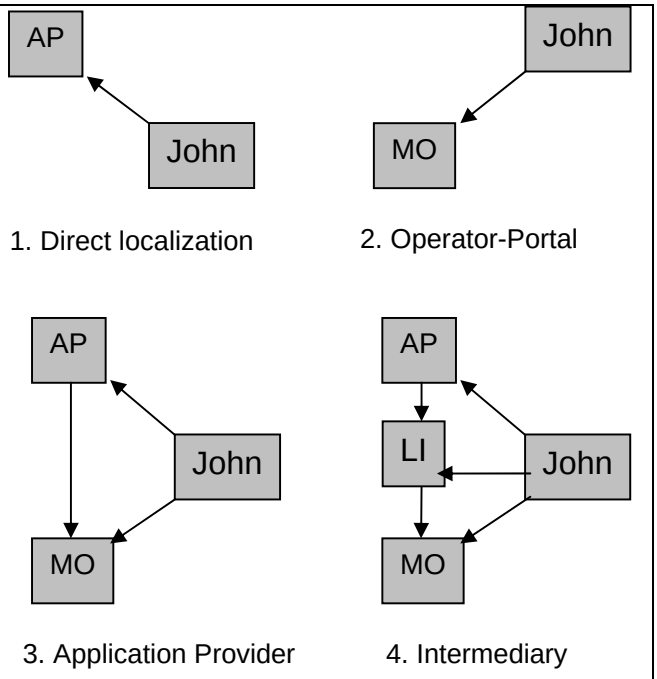

Figure 1: Basic business models for LBS. AP: Application provider; MO: Mobile Operator; LI: Location Intermediary. From [2].

C. *Economic Rationale of the Intermediary Scenario*

The intermediary scenario is the scenario of our choice for a privacy technology specification. The reasons are:

Interoperability An intermediary provides an interface for LBS providers, allowing them to access location data in a unified way.

Multi-channel strategy An intermediary can collect location data from various sources (GSM, WLAN, and GPS).

Synergetic location aggregation An intermediary can aggregate multi-channel location information for the benefit of higher quality (see [3] for an algorithm).

Simplification An intermediary simplifies process handling for LBS providers by removing the need to negotiate contracts with various location sources.

Cross-Operator applications Without an intermediary, the creation of user-to-user LBS with customers using mobile services at distinct mobile operators is much harder.

Pricing advantages Intermediaries provide many economic benefits in information markets, e.g. an intermediary buys location information from location providers in large amounts, and therefore is in a position to negotiate cheaper prices. Intermediary location data might be cheaper to acquire from an intermediary than from a location provider for LBS that consume small amounts of location data. Other benefits of information intermediaries can be found in [4].

II. LBS AND PRIVACY

A. *Economic aspects*

It is often stated that privacy won't sell, and that people will sell their privacy for little but 'immediate gratification'. Nevertheless privacy is a concern of many individuals and privacy legislation exists that manifests these concerns on a national and international level. In [5] Jaisingh et al. examine the effects of different privacy regimes and find evidence that a higher privacy regime increases the efficiency of the exchange of personal identifiable information.

Acquisti distinguishes between on-line identities (pseudonyms) and off-line identities (real world identities). He describes the advantages of using pseudonyms and advocates a more cautious use of real world identities. [6]

B. *New Privacy Threats through LBS*

Location data is data about a person's whereabouts – at a particular time. LBS implement infrastructures that gather this information to compute something with it and send it back to the user or store the result somewhere. Which new privacy threats arise through the observability of someone's location?

1. A subject might find himself or herself in the situation to justify the whereabouts stored in someone else's systems. This is an essential issue concerning control over one's personal data (just like address trade, or consumer profiling).
2. An anonymous subject's identity can be learned by observing its frequently-used locations (where one stays every night is one's home).
3. A subject's context can be guessed by observing location combined with geographic metadata (e.g. about office location, business district, sport locations, red light area).
4. The proximity to other subjects can reveal personal relationships.

Some of these threats can be extended to broad scenarios, e.g. mobile, context- and profile-based spamming of mobile telephone users. Thus, reasoning about protection of location information can be considered useful research. A model for some of these threats can be found in [7].

C. *Technology*

Privacy enhancing technologies (PET) provide pseudonymity, anonymity and identity management in LBS.

Federrath [8] proposed the use of a trusted fixed station and MIXes [9] for hiding the linkage of real world identities to location data in today's mobile telephone networks.

Researchers started to develop LBS specific PETs called mix-zones (see [10] and [7]). Their findings allow for switching location pseudonyms securely.

Anonymity and pseudonymity are only two aspects of privacy. Additionally, control over the flow of information, policies, and user consent have to be considered. Myles et al. investigated the use of a middleware server for evaluating policy rules [11] and Snekkenes [12] identifies concepts for formulating such policies. In [2], Koelsch, Fritsch, Kohlweiss and Kesdogan demonstrate an architecture for LBS with intermediaries that support fine-grained policy expression and enforcement by the mobile user.

Usually consent is expressed by accepting the privacy policy of a service. This process may be automated by comparing the privacy policy of the service with the privacy preferences of their users. But explicit user consent may be a hard requirement in many legal systems before location data can be disclosed.

D. User Expectations

Research in sociology and psychology produced results about users' attitudes, assumptions and requirements concerning privacy in on-line environments. Relevant facts have been found by Kim Sheehan in [13], where four groups of consumers are found to exist: unconcerned Internet users, circumspect Internet users, wary Internet users, and alarmed Internet users. In [14], survey research found that besides the FTC's fair information practices for e-commerce [15], consumers worry about three more issues: consumer control over information-collection, information exchange between companies, and relationship towards the collector of personal information.

Concerning the information to be protected Gary Marx proposes in [16] seven distinct dimensions of personal identity, where location references are one dimension.

Little work has been done to assess LBS specific privacy concerns. Barkhuus and Dey found out in [17] that tracking services are perceived far more intrusive by users than other position-aware services.

III. ID MANAGEMENT , LBS AND THE ECONOMY

M-Commerce applications need to process user identities along their service provisioning. LBS in particular need to process IDs at several components of the infrastructure. My argument here is for the case of LBS that involve mobile operators as the source for location.

A. LBS-specific Identities

First, a mobile phone service subscriber is identified, usually by the SIM card[1] in the phone. The network decides about credibility of the SIM's owner and grants access. Usually, the SIM is mapped to a person's customer record at MO.

Second, the user of the mobile phone uses a mobile data connection to contact a LBS AP. For any permanent business relationship between AP and user, identification has to occur. Now there are three identities involved – the SIM ID, the MO subscriber ID and the customer ID for the LBS AP.

Third, the AP might involve an intermediary for location data and other LBS specific services. The intermediary will contact the users' MO to gather the respective location data. Thus, the intermediary must know who it is doing business for (the AP ID), which MO to contact about the location of the user, and what session of AP is waiting for the result. Now we have a fourth identity represented at the intermediary.

Fourth, and to complicate things further, if you imagine a scenario where LI must show a credential to MO to gather location data, then thee might even be more identity information involved.

B. M-Commerce Identities

Beyond the LBS specific identities to manage, a business scenario usually processes more personal information about its customer relationships. Examples are:

- Delivery address
- Payment information
- Credit history
- Criminal record
- Under age / legal age
- Customer purchase history
- Customer preferences
- CVs about education and job experience

This data, often called profiles, is valuable to businesses for various purposes. Profiles are worthless in case they can't be matched with an identity. Thus, many businesses rely upon some ID along with their customer profiles. In the mobile communications business, the customer ID is very valuable information, as mobile operators have the monopoly on "decoding" the customer relationship of a SIM, and the monopoly of mediation of communication towards the mobile phone the SIM is in. Thus, the control over ID and reach ability provide mobile operators with a strong position in the market, deciding about success or failure of business models. This advantage can be used to implement various business strategies, e.g. discriminatory pricing, bundling, whole selling or locking-in. Any identity management system for LBS privacy seeking market success hence must either convince the legislative or consider the market scenarios for identities.

IV. TOWARDS MOBILE IDENTITY

In this section, I provide some questions and thoughts about mobility and identity with respect to LBS. The first question is about the importance of location. Clearly, location constitutes a context which can be used to deploy a context-based service.

Gary Marx clearly defines locatability as one of his seven dimensions of identity: *"(..) identification can refer to a person's address. This involves location and "reach ability",*

[1] **S**ubscriber **I**dentification **M**odule – a smart card holding network and user identification in mobile telephony networks.

whether in actual or cyberspace (a telephone number, a mail or E-mail address, an account number). This need not involve knowing the actual identity or even a pseudonym. But it does involve the ability to locate and take various forms of action such as blocking, granting access, delivering or picking up, charging, penalizing, rewarding or apprehending. It answers a "where" rather than a "who" question. This can be complicated by more than one person using the same address." (in [16]). This section presents an interesting thought: identifiers like location are only of value if the reach ability of the subject they belong to is provided.

Consideration of [18] reveals the identity paradigm of the Privacy Enhancing Technology community: "*Identifiability is the possibility of being individualized within a set of subjects, the identifiability set. (…) An identity is any subset of attributes of an individual which uniquely characterizes this individual within any set of individuals. So usually there is no such thing as "the identity", but several of them.*". According to this definition, location is just a mere attribute of an identity.

But location changes quickly. Obviously, some attributes are less volatile than others. How will identity management deal with this volatility? Does the concept of mobility put new requirements on the model of identity?

What is a "mobile identity", then? The attribute model obviously needs a freshness concept to be able to distinguish fresh from expired attributes. I do not mean to express that old location attributes are worthless in profiles, but if the fact they're old is not known to the application, confusion may be created to its users. Freshness introduces time into the set of attributes. Thus, a "mobile identity" could be a form of identity that is unique even though location and time attributes can change at will. The challenge of mobile identity management in LBS then is to find a way to provide a certain amount of identity control to the subjects, but at the same time provide reach ability and re-identifiability for the user-to-application provider connection. Clearly, most of the privacy threats identified above result from a combination of a location and time attribute with other attributes, or with a context of the whereabouts (e.g. "This location is within the red light district").

V. Conclusion

A solution for privacy-friendly LBS with identity management has to hide as many attributes from observers as possible, as the location information has to be available to the application provider for provisioning of the service. At the same time, reach ability of the user enables business transactions at all. Thus, the combination of attribute-hiding identity management with untraceable reach ability (e.g. with anonymous channels in a MIX network) are a solution for privacy-friendly LBS. If these two properties are to be implemented in a way supporting the business models presented above, the location-based services can be equipped with privacy-respecting technologies. This assures users they have control over personal data release and identification, as required in the survey research presented above. The most privacy-aware group in Sheehan's typology [13] could possibly be convinced to use mobile on-line services, providing industry a base of usually older, more mature and financially attractive customers who care about privacy.

References

[1] G. Camponovo and Y. Pigneur,Business model analysis applied to mobile business,ICEIS 2003,2003.

[2] T. Koelsch, L. Fritsch, M. Kohlweiss and D. Kesdogan, *Privacy for Profitable Location Based Services*. Berlin: Springer,2005.

[3] J. Myllymaki and S. Edlund,Location Aggregation from Multiple Sources, Proceedings of the Third International Conference on Mobile Data Management (MDM 2002),Singapore,2002.

[4] F. Rose, *The economics, concept and design of information intermediaries*. Heidelberg: Physica-Verlag,1999.

[5] J. Jaisingh, S. Metha and A. Chaturvedi,Privacy and Information Markets: An experimental study,PACIS,Shanghai,2004.

[6] A. Acquisti, "Privacy and Security of Personal Information," in *The Economics of Information Security*, J. Camp and R. Lewis, Ed. Kluwer, 2004,.

[7] M. Gruteser and D. Grunwald,Anonymous usage of location-based services through spatial and temporal cloaking,First International Conference on Mobile Systems, Applications, and Services (MobiSys'03),2003.

[8] H. Federrath, *Sicherheit mobiler Kommunikation: Schutz in GSM-Netzen, Mobilitätsmanagement und mehrseitige Sicherheit.* Braunschweig [u.a.]: Vieweg,1999.

[9] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*. vol. 4, pp. 2 1981.

[10] A. R. Beresford and F. Stajano, "Location Privacy in Pervasive Computing," *IEEE Pervasive Computing*. vol. 2, pp. 46-55, 1 2003.

[11] G. Myles, A. Friday and N. Davies, "Preserving Privacy in Environments with Location Based Applications," *IEEE Pervasive Computing*. vol. 2, pp. 56-64, 1 2003.

[12] E. Snekkenes,Concepts for personal location privacy policies,3rd ACM Concerence on Electronic Commerce,Tampa, Florida, USA,2001.

[13] K. Sheehan, "Toward a Typology of Internet Users and Online Privacy Concerns," *The Information Society*. vol. 18, pp. 21-32, 1 2002.

[14] K. B. Sheehan and M. Grubbs Hoy, "Dimensions of Privacy Concern among Online Consumers.," *Journal of Public Policy & Marketing*. vol. 19, pp. 62-73, 1 2000.

[15] *Privacy Online: Fair Information Practices in the Electronic Marketplace*. 2000.

[16] G. Marx, "What's in a name?" *The Information Society*. vol. 15, pp. 2 1999.

[17] L. Barkhuus and A. Dey, "Location Based Services for Mobile Telephony: a study of users' privacy concerns," 2003.

[18] A. Pfitzmann and M. Hansen, *Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology*. Springer Verlag,2003.

Lothar Fritsch was born in Germany in 1970. He completed his diploma degree in Computer Science with IT security and cryptography focus in 1999 at the Universität des Saarlandes in Saarbrücken, Germany. From 1995 to 1996 he studied Computer Science and Journalism at the University of Missouri in Columbia, Missouri, USA.

He worked as a Product Manager for IT security solutions at fun communications GmbH in Karlsruhe, Germany from 1999 to 2002. There, he developed and marketed certified security solutions and e-signature platforms.

Since 2002, he is a researcher at Johann Wolfgang Goethe-Universität in Frankfurt, Germany. At the chair for Mobile Commerce and Multilateral Security, he develops privacy-respecting M-Commerce technology for real-world business models.

He additionally is a member of Germany's Gesellschaft für Informatik (GI), and the Volcanic Hazards Docmentation and Logistics Research (VHDL).